등차수열을 이용한 효율적인 RFID 인증 프로토콜에 관한 연구

강수영*, 이임영
*순천향대학교 컴퓨터학부
e-mail : bbang814@sch.ac.kr

A Study on Efficient RFID Authentication Protocol using Arithmetic Sequence

Soo-Young Kang*, Im-Yeong Lee
*Division of Computer, SoonChunHyang University

요 약

최근 유비쿼터스와 관련하여 핵심 요소 기술로 활용되고 있는 ad-hoc네트워크와 소형 디바이스에 대한 연구가 활발히 진행되고 있다. 이중 소형 디바이스와 관련해 대표적인 기술이 RFID기술이다. RFID 기술의 특징은 주파수 통신을 이용하여 빠른 인식과 데이터 저장이 가능해 기존의 바코드 기술을 대체할수 있는 새로운 형태의 인증 기술이다. 그러나 RFID의 특성상 소형화된 하드웨어와 주파수 통신을 이용할 경우 보안상 많은 취약성이 존재할 수 있다. 따라서 본 논문에서는 기존의 RFID 기술을 분석한 뒤 보안적 취약성을 보완할 수 있는 등차수열을 이용한 안전하고 효율적인 RFID 인증 기술을 제안하고자 한다. 제안된 방식의 경우 등차수열을 이용함으로서 기존의 방식보다 연산량에 따른 효율성을 유지하면서 기존의 방식의 보안 취약성 보완할 수 있는 방식을 제안하고자 한다.

1. 서론

최근 인터넷 및 정보 통신 기술의 발전으로 인하여 유비쿼터스(Ubiquitous) 환경이 조성되고 있다. 유비쿼터스란 언제, 어디서나 컴퓨팅 디바이스가 있는 곳이라면 서비스를 제공 받을 수 있는 IT 기반 요소를 의미한다. 따라서 유비쿼터스 환경이 구축될 경우 사용자 주변의 낮은 소비전력으로 데이터를 주고받아 안전하게 인식하는 기술이 반드시 요구된다. 이러한 요구에 따른 기술로서 RFID 기술이 주목을 받고 있다.

RFID(Radio Frequency IDentification)란 무선 주파수 인식 기술로서 태그와 리더, 데이터베이스로 구성되어 있다. 태그에 사용자 정보를 저장하고 리더에 의하여 그 정보를 읽히게 된다. 리더는 태그의 정보를 읽어 데이터베이스로 전송하고 인증을 받거나 정보를 관리하게 된다. 이러한 RFID 기술은 저전력이며 소형화된 디바이스로 금융, 의료, 교통, 문화 등 많은 분야에 응용되고 있다.

그러나 RFID 기술은 무선 주파수 기술로써 도청이 가능하다는 문제점을 가지고 있다. 따라서 RFID 시스템에서의 보안에 관한 연구의 중요성이 대두되고 있다. 리더와 데이터베이스 간의 통신 채널은 안전한 채널로써 전송되는 정보가 안전하지만 태그와 리더 간의 통신 채널은 무선 주파수 통신을 하므로 불안전한 채널이다. 따라서 태그와 리더 간의 보안 프로토콜에 관한 연구가 반드시 필요하다.

본 논문에서는 등차수열을 이용하여 RFID 시스템에서의 정당한 개체임을 인증하는 프로토콜을 제안하고자 한다. 2장에서는 인증 프로토콜에서의 요구사항에 관하여 알아보고 3장에서는 기존 프로토콜에 관하여 분석하며 4장에서는 제안 프로토콜에 관하여 기술한다. 마지막으로 5장에서 결론 및 향후 연구 방향에 대하여 논의한다.

2. 위협 요소 및 요구사항

RFID 시스템에서 태그와 리더는 무선 주파수 기술을 사용하기 때문에 많은 공격을 당할 가능성을 가지고 있다. 무선 주파수 통신 채널에서의 도청으로 인한 데이터 위조 및 변조를 방지하고 공격을 당했을 경우에도 이에 대응할 수 있는 방안에 대한 연구가 반드시 필요하다. 따라서 RFID 시스템에서 발생할 수 있는 위협 요소에 대하여 알아보고 이에 대응하여 보안 프로토콜이 갖추어야 할 보안 요구 사항에 대하여 정의하겠다.

2.1 RFID 시스템의 위협 요소

RFID 시스템은 무선 주파수 통신으로 다음과 같은 위협요소를 가지고 있다.

- 도청(Eavesdropping) : 태그와 리더의 통신 채널에서는 무선 기술을 사용하므로 공격자가 쉽게 전송되는 정보를 획득하는 공격 유형이다.
- 트래픽분석(Traffic Analysis) : 태그의 정보를 직접 노출시키지 않더라도 도청된 태그의 응답 값들을 종합하고 분석하여 정보를 획득하는 공격 유형이다.
- 재전송공격(Replay Attack) : 태그의 응답 값이 고정되어 있거나 예측 가능할 때 그 값을 다시 전송함으로써 정보를 획득하는 공격 유형이다.

2.2 RFID 시스템의 요구 사항

RFID 시스템은 다음과 같은 보안 요구 사항을 만족하여야 한다.

- 인증(Authentication) : 어떠한 객체가 정당한 객체인지 모르는 상황에서 정당한 객체만이 획득하거나 생성할 수 있는 값을 전송함으로써 정당하다는 것을 인증 받아야 한다.
- 무결성(Integrity) : 전송되는 태그의 정보에 대해서 전송되는 도중에 위조 및 변조되지 않았다는 것을 증명해야 한다.
- 기밀성(Confidentiality) : 정당한 객체만이 비밀값을 공유해야 한다.
- 효율성(Efficiency) : 저가의 수동형 태그에서의 연산 가능해야 한다.

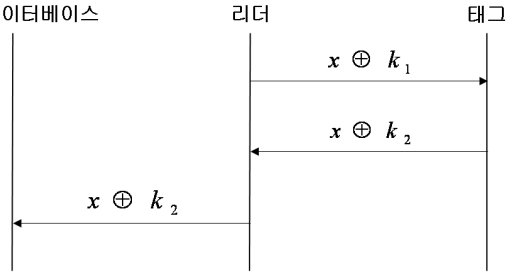
3. 기존 방식 분석

본 장에서는 RFID 시스템의 프라이버시를 제공하는 기존 방식들에 대해서 분석하겠다.

3.1 Lightweight 인증 프로토콜

본 방식은 태그의 제한된 계산 능력과 저장능력을 고려하여 제안한 보안 프로토콜이다. 가정 사항으로 태그는 해쉬 함수를 포함하며 해쉬 연산이 가능하다. 또한 통신이 시작되기 전에 정당한 개체만이 $k^{(0)}$와 $k^{(1)}$을 공유한다[3].

통신이 시작되면 리더는 태그에게 n비트의 랜덤 신호 x와 k_1을 XOR 연산한 값을 전송한다. 키 값은 $k^{(0)}$와 $k^{(1)}$을 XOR한 값으로 태그는 리더로부터 전송되어 온 $k_1 = k^{(0)} \oplus k^{(1)}$을 검증하고 랜덤 신호 x를 획득한다. 태그는 검출한 x에 $k_2 = k^{(0)} \oplus k^{(1)}$를 XOR 연산하여 $x \oplus k_2$를 리더로 전송하고 리더는 태그로부터 전송된 값을 데이터베이스에 전송한다. 데이터베이스는 k_2를 생성한 후 XOR 연산하여 태그에 전송한 랜덤 신호 x를 확인하고 올바른 값이 전송된 경우 태그를 인증한다.



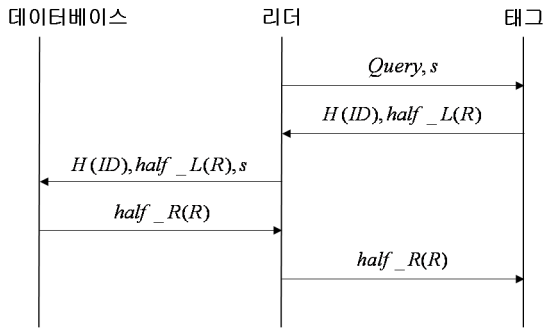
(그림 1) Lightweight 인증 프로토콜

본 방식에서 사용되는 키 값은 One-Time-Pad로 k_1은 이전 세션의 키 값 $k^{(0)}$과 현 세션의 키 값 $k^{(1)}$을 XOR 연산하여 식 $k^{(i-1)} \oplus k^{(i)}$에 따라 생성된다. XOR 연산만으로 보안을 제공하기 때문에 경량화 면에서는 우수하지만 이전 세션의 키 값과의 XOR 연산으로 현 세션의 키 값이 생성되므로 다음 세션의 키 값을 트래픽 분석을 통해 도출할 수 있으며 재전송공격이 가능하다. 또한 데이터가 전송 도중에 위조 및 변조되지 않았다는 것을 확인할 수 없으므로 무결성을 제공하지 못한다.

3.2 Low-Cost 인증 프로토콜

Low-Cost 프로토콜은 저가의 태그에서 연산 가능하도록 제안된 방식으로 태그는 해쉬함수, 리더기는 의사난수생성기(R.N.G)를 포함하고 있다고 가정한다[6, 7].

이 기법에서의 인증 과정은 (그림 2)와 같다. 우선 리더기는 태그에게 $Query$와 의사 난수 생성기를 이용하여 생성한 랜덤수 s를 연접하여 전송한다. s를 전송 받은 태그는 R과 $h(ID)$를 생성하며 R 값은 ID와 s를 연접한 후 해쉬하여 계산한다. R 값은 세션이 다 끝난 후, ID 값을 갱신하기 위해 사용되며 데이터베이스와 태그가 서로 같은 R을 생성했는지 확인하기 위해 사용된다. 이러한 R 값은 반으로 나뉘어 $half_L(R)$과 $half\_R(R)$)로 분리된다. 태그는 $h(ID)$와 $half_L(R)$을 연접하여 리더기에게 전송한다. 리더기는 태그로부터 받은 정보에 s를 같이 데이터베이스에 전송한다. 데이터베이스에서는 $h(ID)$를 통해 태그의 정보를 확인하고, ID와 s를 이용하여 R을 생성한다. 생성된 R과 리더기로부터 전송받은 $half_L(R)$이 같다면 태그를 정당하다고 판단하고 자신의 인증을 위해 $half_R(R)$을 전송한다. 이와 함께 데이터베이스는 R을 통해 ID를 갱신하고 저장한다. 리더기는 데이터베이스로 받은 정보를 태그에게 전송하며 태그는 리더기로 받은 half_R(R)을 비교한 후 같다면 태그도 ID를 $ID \oplus (R \| R)$로 갱신한다. 즉 ID를 변형시켜 프라이버시를 보장하고 재전송공격과 트래픽분석에 안전할 수 있다. 하지만 전의 세션의 안전하게 종료되지 않았다면 태그에서 $h(ID)$로 같은 데이터가 출력되기 때문에 사용자의 위치 확인이 가능하게 된다.



(그림 2) Low-Cost 인증 프로토콜

4. 제안 방식

본 장에서는 기존 인증 프로토콜에 관한 연구들을 기반으로 분석한 취약점에 대하여 보완하고 요구사항에 따른 프로토콜을 제안한다.

4.1 가정 사항

본 제안 방식은 다음과 같은 가정 사항을 기반으로 수행된다.

① 사전 단계에 정당한 객체만이 K_0와 K_1를 안전하게 공유한다.
② 태그는 해쉬 연산과 XOR 연산을 수행할 수 있으며 각각의 태그는 유일한 ID를 가지고 있다.
③ 태그는 One-Time-Pad로 키 갱신이 이루어지며 갱신된 키는 그 세션에서만 사용된다.
④ 리더는 R.N.G(Random Number Generator)를 가지고 있어 랜덤수를 생성할 수 있다.
⑤ 리더는 정당한 객체로 데이터베이스와의 채널이 안전하다.

4.2 시스템 계수

본 제안 방식에 사용되는 시스템 계수는 다음과 같이 정의한다.

- $H(\ )$: 해쉬 연산한 값
- K_0 : 정당한 객체만이 공유한 초기 키 값
- K_1 : 정당한 객체만이 공유한 초기 키 값
- S : K_0와 K_1의 차로서 세션키 값
- M : K_0와 K_1의 합으로서 세션키 값
- ID : 태그의 식별 값
- SID : 태그의 가상 ID로 매 세션 갱신되는 값으로 $ID \oplus r$로 구성
- K_{MID} : S와 M의 등차중앙
- R_K_{MID} : 등차중앙의 오른쪽 8비트
- L_K_{MID} : 등차중앙의 왼쪽 8비트
- r : 리더에서 생성한 랜덤수
- $count$: 태그의 세션 번호
- $\oplus$: XOR 연산

4.3 제안 방식 프로토콜

본 방식은 등차수열을 응용하여 RFID 시스템에서의 인증 프로토콜을 제안한다. 재전송공격에 안전하며 추적 문제에도 안전한 프로토콜로써 인증 과정은 다음과 같다.

사전단계 : 정당한 개체인 데이터베이스와 리더, 태그들은 K_0와 K_1을 공유한다. 또한 태그의 $count$ 값을 확인한다.

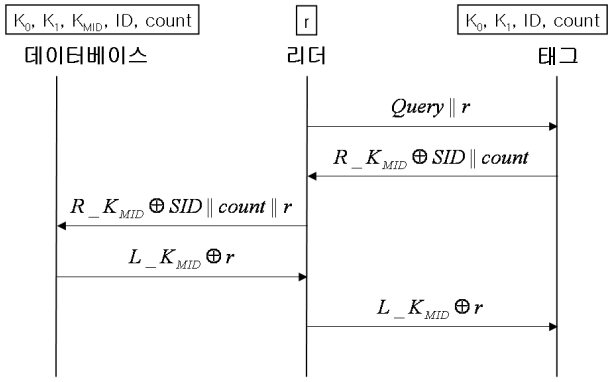
① 리더는 태그에게 통신을 시작하기 위한 신호인 $Query$와 리더에서 생성한 랜덤수 r을 연접하여 태그에 전송한다.

$$Query \| r$$

② 태그는 자신이 가진 K_0와 K_1를 이용하여 두 키 값의 차와 합인 S와 M을 계산하고 두 값의 등차중앙인 K_{MID}를 생성한다. 등차중앙 K_{MID}를 반으로 오른쪽 8비트와 왼쪽 8비트로 분리하고 오른쪽 8비트와 왼쪽 8비트를 패딩하여 16비트 데이터를 생성한다. 그 후 SID를 XOR 연산하여 $R_K_{MID} \oplus SID$를 생성하고 세션의 횟수인 $count$를 연접하여 $R_K_{MID} \oplus SID \| count$를 리더에 전송한다. 등차중앙 K_{MID}와 SID 및 S, M의 연산식은 다음과 같다.

$$K_{MID} = (S + M)/2$$
$$SID = ID \oplus r$$
$$S = K_1 - K_0$$
$$M = K_1 + K_0$$

③ 리더는 태그로부터 $R\_K_{MID} \oplus SID \| count$ 값을 전송받고 랜덤수 r을 연접하여 데이터베이스에 전송한다. 데이베이스는 $count$에 해당하는 등차중앙의 오른쪽 8비트와 리더로부터 전송된 랜덤수 r 그리고 두 키의 합과 차를 이용한 S와 M을 $R\_K_{MID} \oplus SID$ 값에 XOR 연산하여 ID를 획득한다. 획득한 ID를 데이터베이스에서 검색하여 일치하는 정보가 있을 경우 태그를 인증한다.



(그림 3) 제안 방식

④ 데이터베이스는 태그 인증 후 등차중앙의 왼쪽 8비트와 랜덤수 r을 XOR 연산하여 리더에 전송한다.

⑤ 리더는 $L\_K_{MID} \oplus r$ 값을 태그에게 전송하고 태그는 리더로부터 전송된 값을 검증한다. 등차중앙의 왼쪽 8비트 L_K_{MID}와 랜덤수 r을 연산하여 $(S \oplus M)/2$을 생성한 후 $L\_K_{MID} \oplus r$ 값과 비교하여 일치할 경우 전송된 값을 검증한다. 올바른 값으로 판단되어질 경우 데이터베이스를 인증하고 태그의 키 값은 S와 M으로 갱신한다. 또한 태그의 세션 번호인 $count$를 1 증가시키고 인증 과정을 종료한다.

4.4 제안 방식 분석

본 제안 방식은 등차수열을 기반으로 하여 기존 방식의 취약점을 보완하여 효율적인 보안 프로토콜을 제안하였으며 기존 방식과의 비교를 [표 1]과 같이 분석하였다.

- 인증 : 데이터베이스는 세션의 횟수인 $count$와 랜덤수 r을 사용하여 획득한 ID를 데이터베이스에서 검색하고 일치하는 정보가 있을 경우 태그를 인증한다. 태그는 등차중앙의 왼쪽 8비트와 랜덤수 r을 XOR 연산하여 데이터베이스로부터 전송된 데이터 $L_K_{MID} \oplus r$을 생성하고 비교 후 값이 일치하면 데이터베이스를 인증한다.
- 무결성 : 데이터베이스가 리더로부터 전송된 값을 검증하기 위해서 등차중앙의 값을 생성하여 비교하고 SID를 ID와 r을 XOR 연산하여 검증하므로 통신에 사용되는 값들이 전송 도중에 위조 및 변조 되지 않았다는 것을 검증할 수 있다.
- 기밀성 : 사전 정당한 객체만이 비밀키 값 K_0과 K_1은 공유하므로 두 키를 가지고 있는 객체만이 인증 받을 수 있으며 기밀성을 제공한다.
- 효율성 : XOR 연산만을 사용하여 사용자 프라이버시를 안전하게 하며 데이터베이스에서 ID를 효율적으로 검색할 수 있기 때문에 태그의 효율성 및 데이터베이스의 효율성을 제공한다.

[표 1] 제안 방식의 비교 분석

	Light weight	Low-Cost	제안 방식
도청	가능	불가능	불가능
트래픽분석	가능	가능	불가능
재전송공격	가능	불가능	불가능
인증	제공안함	제공함	제공함
무결성	제공안함	제공함	제공함
기밀성	제공안함	제공함	제공함
효율성	제공함	제공함	제공함

5. 결론 및 향후 연구 방향

다가오는 유비쿼터스 환경에서는 금융, 의료, 교통 문화 등 다양한 서비스가 제공될 것이며 정당한 사용자가 서비스를 제공 받기 위해서는 사용자 개인 정보를 노출이 불가피하다. 그러나 이러한 사용자 정보 유출로 개인의 프라이버시 위협이 따르게 된다. 따라서 프라이버시 문제를 해결하기 위해 본 논문에서는 등차수열 알고리즘을 응용하여 사용자 프라이버시를 안전하게 보호하고 수동형 태그에서 연산 가능할 수 있도록 구현된 효율적인 보안 프로토콜을 제안하였다.

보안 프로토콜에서 전송되는 데이터에 난수의 사용과 많은 연산으로 수학적 요소는 항상 포함되기 마련이다. 따라서 본 논문은 일정한 수를 더해가는 등차수열 알고리즘을 응용하여 두 수의 중간 값인 등차중앙 값을 응답 값으로 전송함으로써 불법적인 공격자가 정당한 객체로 인증 받을 수 없도록 하였다. 본 방식은 두 개의 키 갱신과 랜덤수를 사용하므로 트래픽분석 및 재전송공격에는 안전하지만 마지막 통신이 정상적으로 종료되지 않았을 경우 위치 추적에 안전하지 않을 수 있다. 따라서 향후 경량화된 프로토콜만으로 위치 추적으로부터 안전할 수 있는 방안에 관한 연구가 이루어 져야 할 것이다.

참고문헌

[1] Damith C.Ranasinghe, Daniel W.Engels, Peter H.cole, "Low-Cost RFID Systems : Confronting S-ecurity and Privacy", Auto-ID Lab Research Wo-rkshop, 2004.09

[2] Dirk Henrici, Paul Muller, "Hash-based Enhan-cement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers", Workshop on Pervasive Computing and Communi-cations Security - PerSec, 2004.03

[3] Istvan Vajda, Levente Buttyan, "Lightweight Authentication Protocols for Low-Cost RFID Tags", Workshop on Security in Ubiquitous Computing, 2003.08

[4] Miyako Ohkubo, Koutarou Suzuki, Shingo Kin-oshita, "Cryptographic approach to 'Privacy-Frie-ndly' Tags", RFID Privacy Workshop, 2003.11

[5] Tassos Dimitriou, "A Lightweight RFID Protoc-ol to Protect Against Traceability and Cloning A-ttacks", Conference on Security and Privacy for Emerging Areas in Communication Networks-Sec ure Comm, 2005.09

[6] 박장수, 이임영, "RFID에서의 안전한 상호인증 프로토콜에 관한 연구", 2005년 멀티미디어학회 춘계학술발표대회 논문집 p520~523

[7] 황영주, 이수미, 이동훈, 임종인, "유비쿼터스 환경의 Low-Cost RFID 인증 프로토콜", 2005년 정보보호학회 하계정보보호학술대회 논문집 p109~114